NSX Advanced Load Balancer (Avi Networks) Web Application Firewall (WAF)

Modern App Security with Point-and-Click Simplicity

CHALLENGES

- Increasing complex process for writing security policies and rules
- Lack of visibility into how policies impact traffic flows
- Low performance and massive variability result in scaling and capacity planning challenges

SOLUTION — AVI WAF

- Real-time visibility and insights into application performance, end-user experience and security patterns
- Elastic horizontal autoscaling to handle security attacks and easy rule generation to customize response
- GDPR, HIPAA, and PCI compliance with config audit trail across a distributed software fabric

BENEFITS

- Point-and-click simplicity for policies with central security management
- Granular security insights on traffic flows and rule matches to create precise and custom policies
- Elasticity with on-demand autoscaling, optimized security pipeline and per-app protection

WEB APPLICATIONS ARE UNDER-SECURED BY TODAY'S WAFs

Web application firewalls (WAFs) are intended to protect businesses from web app attacks and proactively prevent threats. Yet, despite the potential security benefits, 90% of organizations find it complex to implement WAF solutions for three key reasons:

- Complex rules. Most WAFs today are very complicated, presenting a wall-of-knobs to administrators in order to configure security policies. Tuning rules is even more challenging, not to mention customizing for each application.
- No visibility or intelligence. Most WAFs today provide little visibility and lack attack behavior modeling and application learning. Once rule sets are defined, it is difficult to update, monitor and impossible to react in real time to changes or new security threats.
- Slow to scale. Traditional WAFs are inelastic and unable to provide the scalability required for increasing volumes of encrypted traffic and variable loads. Hardware appliance based WAFs need significant overprovisioning.

OPERATIONAL INTELLIGENCE THROUGH MACHINE LEARNING

Avi features an intelligent Web Application Firewall (WAF) with a distributed application security fabric to enforce security through closed-loop analytics and application learning mode. The built-in solution provides security and networking teams with a comprehensive app security stack including WAF, DDoS, rate limiting, SSL/TLS encryption, user authentication, ACL and bot management pipeline that simplifies policy customization and scales automatically on-demand across any environment. WAF covers OWASP CRS protection, support for compliance regulations such as PCI DSS, HIPAA, and GDPR, allow list operations, positive security model, and signature-based detection. Bot management covers bot detection, classification and actions that need to be taken to control the behavior of bots that have been classified. See Figure 1.

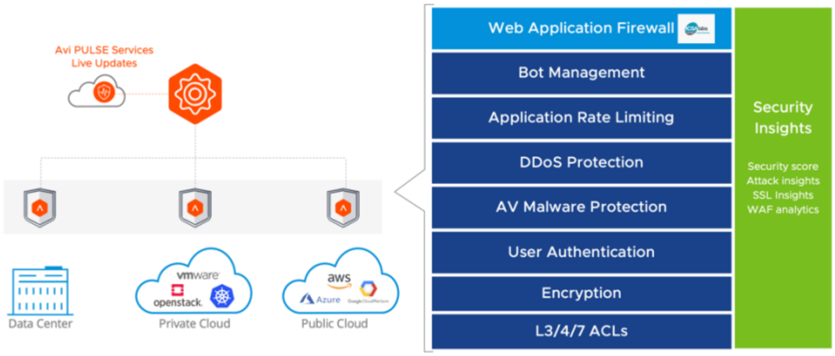

FIGURE 1: Application Security/WAF Comprehensive Security Stack

Avi offers malware protection and content sanitization capabilities (see Figure 2) through ICAP (Internet Content Adaptation Protocol) integrations with anti-malware technologies including OPSWAT and Lastline (now part of VMware). The ICAP integrations enable real-time inspection of web traffic for malware and vulnerabilities. Policies and configured workflows enable file blocking and removal or redactions of sensitive information before leaving the network.

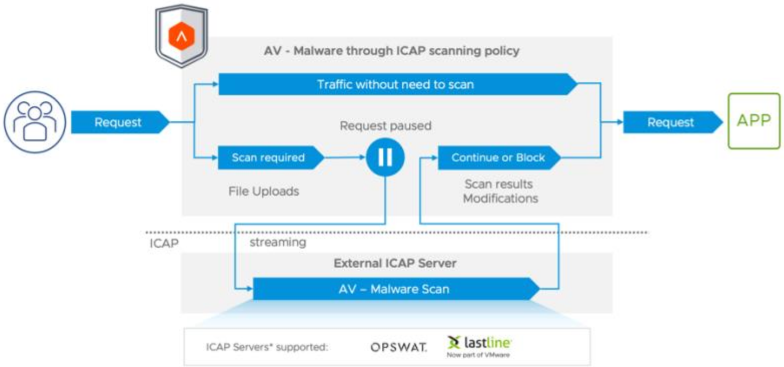

Figure 2: Avi's Antivirus Malware Protection

Avi's WAF gives administrators end-to-end security insights and analytics on performance, end-user interactions and security events in a single dashboard (Avi App Insights) for actionable insights on security intelligence and enforcement. With Avi PULSE Services, live threat updates including IP reputation, signatures and more are sourced from industry leading threat analysis companies and curated through the Avi PULSE. It protects web applications from common vulnerabilities, such as SQL Injection (SQLi) and Cross-site Scripting (XSS), while providing the ability to customize the rule set for each application. WAF analyzes the unvalidated traffic through the allow list engine, positive security model that validates known good behavior as applications and attack patterns are learned and lastly, the signatures engine processes security rules that match a particular transaction – all these in real-time. The optimized security pipeline maximizes efficiency, sharply reduces false-positives, and blocks zero-day attacks. See Figure 3.

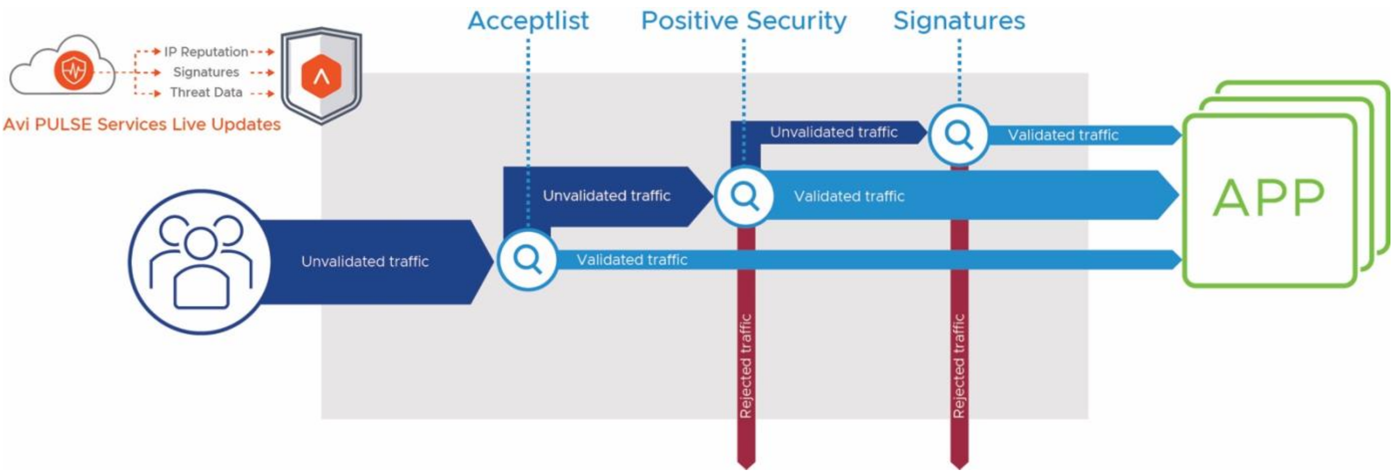

Figure 3: Avi WAF Security Pipeline Optimization

Avi's bot management solution is introduced (as tech preview/beta version) to mitigate bad bots. The solution enables you to filter the bots that should be allowed to access the web assets and the bots that should be rate-limited or blocked. See Figure 4.

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-so-temp-word-103-proof 5/19

Bot management includes:

1. Bot Detection – The request goes through various checks to detect the bots.
2. Bot Classification – The bot is classified as human, good bot, bad bot, etc.
3. Actions – Defined to control the behavior of classified bots (rate limit, allow, close connection, end custom response, etc.).

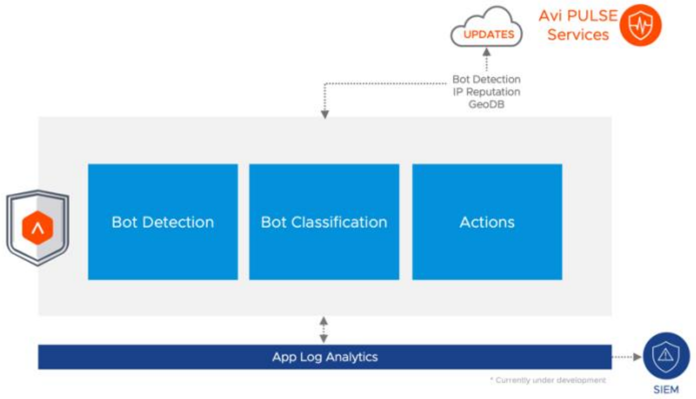

Figure 4: Avi's Bot Management Pipeline

FEATURES AT-A-GLANCE

Core Security

- **OWASP Top 10 attack protection** including HTTP validation, injection, data leakage protection, automated attack blocking and application specific security.
- **Guided false-positive mitigation** with customizable paranoia levels that control the strictness of the policy based on the logs and analytics.
- **Rate-limiting per app** to limit L3/L4 and L7 traffic based on parameters such as Client IP, URL and Path.
- **Point-and-click policy** with central control and ease of use by enabling users to create custom policies quickly and efficiently.
- **RBAC support** to control write access to WAF profiles and policies; read access to applications, pools, and clouds.

Threat Detection

- Allow List rules that allow bypassing WAF with known good sources. E.g: Allow DAST scanner IPs from WAF inspection, to exclude internal IP addresses from WAF inspection or to bypass WAF for all POST requests.
- **Signatures protection** against known threats through a negative security approach by analyzing every part of the incoming and outgoing requests against SQLi, XSS and other threats based on Core Rule Set (CRS).
- **Application Rules** protect against known exploits in 3rd party, open source or closed source applications. Our database tracks over 5000 applications with 15k+ rules. Automatic updates ensure that your applications are always protected.
- **Automated threat updates**. Sourced from industry leading threat analysis companies Avi Pulse Services continuously updates the iWAF thread database with IP reputation, signatures, and more, protecting web applications from common and new vulnerabilities.

Application Protection

- **Positive Security Model** rules define allowed application behavior and can be created automatically by the learning engine through sampling traffic or manually.
- **Per-app deployment** for precision protection of specific applications with different security policy levels while ensuring application performance.
- **On-demand autoscaling** to elastically scale the number of WAF instances and application servers to handle unpredictable traffic without impacting performance.
- **Application analytics** for WAF events based on historical trend information and real-time visibility into ongoing operations, application behavior analysis, and attack patterns.
- **Bot Management** to detect bot traffic, determine its intent, and mitigate bad bots to optimize customer experience, protect digital assets, and prevent online fraud. Bot management is available today as tech preview/beta version only.

Copyright © 2019 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-so-temp-word-103-proof 5/19